Puppet Masters
Pulling the Strings Behind Social Engineering Attacks

Erich Kron
Security Awareness Advocate, KnowBe4, Inc.
Erich Kron
Security Awareness Advocate

About Erich Kron

- CISSP, CISSP-ISSAP, MCITP, ITIL v3, etc…
- Former Security Manager for the US Army 2nd Regional Cyber Center – Western Hemisphere
- Former Director of Member Relations and Services for (ISC)²
- A veteran of IT and Security since the mid 1990’s in manufacturing, healthcare and DoD environments
KnowBe4, Inc.

- The world's most popular integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex- antivirus, IT Security pros
- 200% growth year over year
- We help tens of thousands of organizations manage the problem of social engineering
“All warfare is based on deception.”

- Sun Tzu, *The Art of War*
You never know what’s really going on with the internet
Phishing: By The Numbers
91% of successful data breaches started with a spear phishing attack

- Ransomware is predicted to exceed damages of $11.5 billion and continues to grow
- Spear-phishing emails were used by 71% of attack groups in 2017
- In March 2018, 1 in 484 emails to organizations with 251-500 employees had malware
The Costs of Breaches and Ransomware Attacks

- The average cost of a ransomware attack on businesses was $133,000.
- 75% of companies infected with ransomware were running up-to-date endpoint protection.
- 34% of businesses hit with malware took a week or more to regain access to their data.
CEO Fraud and BEC Causes $26 Billion in Damages

There are various versions of the scams. Victims range from large corporations to tech companies to small businesses to non-profit organizations. Many times, the fraud targets businesses that work with foreign suppliers or regularly perform wire transfer payments.

- Law enforcement globally has received complaints from victims in every U.S. state and in at least 177 countries.
- FBI Alert Number I-091019-PSA puts the losses at over $26 billion between October 2013 and July 2019.
- Between May 2018 and July 2019, there was a 100% increase in identified losses.
Agenda

• The Perception vs. Reality dilemma
• Focus Redirection
• Psychology Applied to Phishing
• How we can defend ourselves and our organizations
Agenda

• The Perception vs. Reality dilemma
• Focus Redirection
• Psychology Applied to Phishing
• How we can defend ourselves and our organizations
Understanding the root of deception

Our brains’ job to filter, interpret, and present ‘reality’
An Interesting History

Using our brain’s strengths against us

Left: Normal expression of face. Right: Exaggerated expression of
dumbness. The more facial muscles are relaxed and eyes thrown out
of focus, the greater the effect. Doing these actions to a mild degree
merely shows a lack of alertness or disinterest.
What is REALITY?

Yanny -or- Laurel?
**Agenda**

- The Perception vs. Reality dilemma
- Focus Redirection
- Psychology Applied to Phishing
- How we can defend ourselves and our organizations
Pick a card!
Is it gone now?
How did we identify and remove your card?

Here’s what we started with:

And here’s what we ended with:

Yeah: These are two completely different sets of cards. But, by rushing you through the process, you probably didn’t notice!
An Interesting History

Using our brain’s strengths against us

Left hand lowered for action immediately after match is struck.
Agenda

- The Perception vs. Reality dilemma
- Focus Redirection
- Psychology Applied to Phishing
- How we can defend ourselves and our organizations
“I’ve never found it hard to hack most people. If you listen to them, watch them, their vulnerabilities are like a neon sign screwed into their heads.”

Elliot Alderson
Attackers will do *anything* to bypass critical thinking

- Spoofs a campus-wide security alert for a community college (confidential information blocked out) in Florida.
- Exploits current concerns over active shooters on education campuses
- Crafted to generate a reflexive click.
- Directs to credential capture site.
- Other variants seen:
  - “IT DESK: Security Alert Reported on Campus”
  - “IT DESK: Campus Emergency Scare”
  - “IT DESK: Security Concern on Campus Earlier”
Example: Business Email Compromise (The Phish Evolved)

- a.k.a. CEO Fraud
- No payload
- Low volume email targeting high value individuals
- Personalized
- Few to no ‘traditional’ spam/phishing tells (such as poor grammar, egregious misspellings, etc.)
Not all scammers are skillful, but some are.

This is not one of them
Example: Gift Card Scams

From: executive@pharma.com
Message-ID: <1758473657.82816.1549554140411@webmail.pharma.com>

----
Hi Liz,
I need you to make a purchase of Itune Giftcard this morning, It's a gift for a vendor, Are you available to make the purchase now?

Best Regards,
Patrick. (edited)
Subject: Eft dd info update
from=pavinski1810991ua@gmail.com
To: (Payroll)
(Payroll),
I 'll like to change my EFT dd info, can it be effective for the current pay date ? My old account is closed and i changed to a new financial institution.
Regards
(CEO) (edited)
Example: Tech Support Scam

** Microsoft Warning Alert **

ERROR # 268d3x8938(3)

Please call us immediately at:
+1-(888)-919-6150 (Toll Free)

Do not ignore this critical alert.

If you close this page, your computer access will be disabled to prevent further damage to our network.

Your computer has alerted us that it has been infected with a Pornographic Spyware and riskware. The following information is being stolen...

1. Facebook Logins
2. Credit Card Details
3. Email Account Logins
4. Photos stored on this computer

You must contact us immediately so that our expert engineers can walk you through the removal process over the phone to protect your identity or from any information loss.

Call Microsoft: +1-(888)-919-6150 (Toll Free)
Example: Wire Transfer Fraud

Step 1:
Starts Simple

Step 2:
Moves to the attack

Source: BEC-international Slack Channel
Blogs That Are Compromised

• Blogs are often compromised and used to host malware.

• Many of the links in emails will look like they go to a legitimate site, but when you hover over the link, it tells a very different story.

https://toprankbuyscash.com/blog/wp-admin/css/colors/blue/
Click or tap to follow link.
Attackers will use images to replace text with an image to hide from security tools that look for words or word patterns.

Passing over the area of the text changes your cursor and lets you spot the link.
Clickbait: It’s More Science Than You Think

• Leverages “pattern interruption” to create curiosity often based on the "information-gap" theory

• “Such information gaps produce the feeling of deprivation labeled curiosity. The curious individual is motivated to obtain the missing information to reduce or eliminate the feeling of deprivation.” - George Loewenstein, Carnegie Mellon

• Also leverages outrage and anger, which drives us to take action
Agenda

- The Perception vs. Reality dilemma
- Focus Redirection
- Psychology Applied to Phishing
- How we can defend ourselves and our organizations
Defense Against The Dark Arts

• Technical
  • Email Gateways
  • SPF/DKIM/DMARC
  • 2FA/MFA

• Non-Technical
  • End-User Training
  • Reporting
Email Gateways

• Filtering email from known bad actors can greatly reduce the sheer volume of emails coming in to an organization.

• These tend to be effective against generic phishing and spam, but less effective against targeted attacks.

• Generally speaking, even the best gateways still pass about 10-15% of the phishing messages.
SPF/DKIM/DMARC

• Sender Policy Framework (SPF) records are an email authentication method designed to detect forged sender addresses through DNS records listing authorized MX servers for the domain.

• DomainKeys Identified Mail (DKIM) is also an email authentication method designed to detect forged sender addresses using PKI and digital message signing.

• Domain-based Message Authentication, Reporting and Conformance (DMARC) records specify if the domain uses SPF and/or DKIM from that domain and what to do if the message fails the SPF or DKIM test.
Multi-Factor Authentication

• While it’s always better to avoid giving up the credentials in the first place, you can use 2-Factor (2FA) or Multi-Factor (MFA) authentication to help mitigate the risks of credential theft.

• Multi-Factor is not fool-proof and can be bypassed, however it is still more secure than a single factor.

• My preference in order of ease of use is as follows:
  • SMS-based
  • Application-based
  • Hardware-based
End User Training and Reporting

- Once trained, users can become very good at spotting these attacks, however they need to be reminded to stay vigilant and kept up to date on new types of attacks.

- Pairing the training with ongoing simulated phishing emails keep them looking for the attacks and allows them to make mistakes in a fail-safe environment.

- Training should avoid being overly technical and instead focus on making the issue relevant to the users.

- Once they are proficient at spotting the attacks, give them an easy method to report the emails. This can become a very useful threat-intel feed that can help you identify when you are targeted by campaigns.
Training Focus Points

Social Engineering

Are You Being Manipulated?
-- understand the lures --

Greed  Curiosity  Self Interest
Urgency  Fear  Helpfulness
Training Focus Points

Social Engineering Red Flags

FROM
- I don’t recognize the sender’s email address, as someone I ordinarily communicate with.
- The email is from someone outside my organization and it’s not related to my job responsibilities.
- The email was sent from someone inside the organization at a false alias, someone, or partner who is very unusual or out of character.
- The sender’s email address is from a suspicious domain (like microsoft-support.com).
- I don’t know the sender personally and they were not vouched for by someone I trust.
- I don’t have a business relationship with any past communications with the sender.
- This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I haven’t communicated with recently.

TO
- I was CC’d on an email sent to one or more people, but I don’t personally know the other people it was sent to.
- I received an email that was also sent to an unusual mix of people. For example, it might be sent to a random group of people or the organization I work for but named starts with the same letter, or a whole list of unrelated addresses.

SUBJECT
- Did I receive an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 am?
- Did I get an email with a subject line that is irrelevant or does not match the message content?
- Is the email message a reply to something I never sent or requested?

DATE
- Did I receive an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 am?

ATTACHMENTS
- The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message. (This sender doesn’t ordinarily send me this type of attachment.)
- I see an attachment with a possibly dangerous file type. The only file types that are always safe to click on are .txt files.

CONTENT
- Is the sender asking me to click on a link or open an attachment to avoid a negative consequence or to gain something of value?
- Is the email out of the ordinary, or does it have bad grammar or spelling errors?
- Is the sender asking me to click a link or open an attachment that seems odd or illogical?
- Do I have an uncomfortable gut feeling about the sender’s request to open an attachment or click a link?
- Is the email asking me to look at a compromising or embarrassing picture of myself or someone I know?

© 2017 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks or registered trademarks of their respective companies.
The users CAN learn, I promise!

- Training once a year won’t do it. It needs to be consistent throughout the year.

- Try the following:
  - Annual training - 45min to an hour
  - Quick ongoing training – 3-5 minutes at least quarterly
  - Simulated phishing attacks – at least once per month

New-school security awareness, coupled with frequent simulated phishing training, will help employees make smarter security decisions, everyday.

![Graph showing Phish-prone Percentage over time](image)

- Initial Baseline Phish-prone Percentage: **AVG 30%**
- 3 Months Later: **AVG 15%**
- 12 Months Later: **AVG 2%**
Build engagement and decrease behavior-related risk

Baseline Testing
We provide baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack.

Train Your Users
On-demand, interactive, engaging training with common traps, live hacking demos and new scenario-based Danger Zone exercises and educate with ongoing security hints and tips emails.

Phish Your Users
Fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.

See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!
Thank You!

Erich Kron – Security Awareness Advocate
ErichK@KnowBe4.com | @KB4Erich | @ErichKron